Data Mining for Fun and Profit: 
Building an Historical Database of Adversary Information 
John Bambenek, Threat Research Team, Fidelis Cybersecurity 
SANS Threat Intelligence Summit, 2016
Introduction

- Threat Instigator with Fidelis Cybersecurity
- CS Faculty at the University of Illinois
- Producer of open-source intelligence feeds
- Run several takedown-oriented groups for various malware families
Shorter Version
The Problem... Illustrated

Virustotal Statistics taken at Jan 16, 2016
China Unable To Recruit Hackers Fast Enough To Keep Up With Vulnerabilities In U.S. Security Systems

BEIJING—Despite devoting countless resources toward rectifying the issue, Chinese government officials announced Monday that the country has struggled to recruit hackers fast enough to keep pace with vulnerabilities in U.S. security systems. “With new weaknesses in U.S. networks popping up every day, we simply don’t have the manpower to effectively exploit every single loophole in their...
TL;DR

Bad News: We’re Doomed

Good News: Unlimited Job Security
Threat hunting

• Lots of talk about hunting threats in your network, but…

• The threats keep coming…
  • Good for vendors, bad for enterprises.
I prefer to hunt the attackers…
My intelligence objective

• I prefer to run operations designed to end a given threat and hopefully put someone in prison.

• This creates intelligence biases that are important to note.
  • i.e. Direct operationalization of data has issues that need resolved.

• Sources of data are external to a given enterprise
  • But we’ll use internal sources too and so should you.
Putting the Intelligence back in Threat Intel

- Information is a set of unprocessed data that may or may not contain actionable intelligence.

- Intelligence is the art of critically examining information to draw meaningful and actionable conclusions based on observations and information.

- Involves analyzing adversary capabilities, intentions and motivations.

- Problem: Threat intel is sold based on quantity, not quality. Intel is hard and takes time.
How to win at VC…

• VirusTotal generally has C2 information (assuming sample runs).

• If vt > 1/55 then dump all network info, apply whitelist (maybe), call it a threat intel feed….

• Collect your $50 million in VC funding.

• Create pew-pew map.

• Apply logo.
How to not suck

• Point-in-time data is of limited use.
  • Data can “expire”
  • Can’t derive any context
  • Can’t determine motivations, capabilities
  • Can’t forecast off a data point

• Need to know when data is no longer any good?
  • Domains suspended
  • Hosting companies clean up compromised sites
  • Infrastructure changes
Two case studies

• Data mining malware
  • Can process about 30 families (many decoders open source)
  • Can correlate off configuration items to find related campaigns

• DGA surveillance
  • Currently running DGA feeds, running for over 2 years
  • Bulk resolving of all domains for information
What can you do with malware configs?

- In fullness of time, I plan to provide a feed to LE and CERTs for remediation.
- Sinkholing for victim notification is a possibility.
- Mining the data for correlations.
- Mine historical database for indicators that didn’t seem important at the time but became important later.
Open source magic sauce...

- [https://github.com/kevthehermit/RATDecoders](https://github.com/kevthehermit/RATDecoders) by Kevin Breen

- Python scripts that will *statically* rip configurations out of ~three dozen different flavors of RATs.

- Actively developed and you can see in action at malwareconfig.com

- Most malware has artifacts and many can be recovered statically.
Malware Sources

• VirusTotal

• MSFT VIA Program

• Other malware sharing programs

• Your own spam **IMPORTANT**

• In total, I process upwards of .25 TB a day

• If you have malware you want to trade, let’s talk.
Malware Configs

• Every malware family has different configurable items.

• Not every configuration item is necessarily valuable for intelligence purposes, some items may have default values.

• Free-form text fields provide interesting data that may be useful for correlation.

• Mutex can be useful for correlating binaries to the same actor.
Sample DarkComet config

Key: CampaignID    Value: Guest16
Key: Domains       Value: 06059600929.ddns.net:1234
Key: FTPHost       Value:
Key: FTPKeyLogs    Value:
Key: FTPPassword   Value:
Key: FTPPort       Value:
Key: FTPRoot       Value:
Key: FTPSize       Value:
Key: FTPUserName   Value:
Key: FireWallBypass Value: 0
Key: Gencode       Value: 3yHVnheK6eDm
Key: Mutex         Value: DC_MUTEX-W45NCJ6
Key: OfflineKeylogger Value: 1
Key: Password      Value:
Key: Version       Value: #KCMDDC51#
Sample njRat config

Key: Campaign ID   Value: 1111111111111111111
Key: Domain       Value: apolo47.ddns.net
Key: Install Dir   Value: UserProfile
Key: Install Flag  Value: False
Key: Install Name  Value: svchost.exe
Key: Network Separator   Value: |
Key: Port         Value: 1177
Key: Registry Value Value: 5d5e3c1b562e3a75dc95740a35744ad0
Key: version      Value: 0.6.4
Sample Output

0739b6a1bc018a842b87dcb95a73248d3842c5de,150213,Dark Comet Config,Guest16,lolikhebjegehackt.ddns.net,1604,o1o5GgYr8yBB,DC_MUTEX-4E844NR

0745a4278793542d15bbdbe3e1f9eb8691e8b4fb,150213,Dark Comet Config,Guest16,ayhan313.noip.me,1604,aWUZabkJRte,DC_MUTEX-TX61KQS

07540d2b4d8bd83e9ba43b2e5d9a2578677cba20,150213,Dark Comet Config,FUDDDDD,bilalsidd43.no-ip.biz,204.95.99.66,1604,qZYsyVu0kMps,DC_MUTEX-8VK1Q5N

07560860bc1d58822db871492ea1aa56f120191a,150213,Dark Comet Config,Victim,cutedna.no-ip.biz,1604, sfAEjhc4m1IQ7,DC_MUTEX-F2T2XKC

07998ff3d00d232b6f35db69ee5a549da11e96d1,150213,Dark Comet Config,test1,192.116.50.238,90,4A 2xbJmSqvuc,DC_MUTEX-F54S21D

07ac914bdb5b4cda59715df8421ec1adfaa79cc7,150213,Dark Comet Config,Guest16,alkozor.ddns.net,31.13 2.106.94,1604,1.ekspert60.z8.ru,################60,############2012,zwd8tEC0F0tA,DC_MUTEX-W3VUKQN

NOTE – Redacted entries are username and password for FTP drop for keyloggers.
OPSEC? What OPSEC?

THE GRUGQ FINDS YOUR LACK OF OPSEC...

DISPLEASING
<table>
<thead>
<tr>
<th>Dark Comet Campaign IDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>11510 Guest16</td>
</tr>
<tr>
<td>1563</td>
</tr>
<tr>
<td>Guest16_min</td>
</tr>
<tr>
<td>924</td>
</tr>
<tr>
<td>125 Kurban</td>
</tr>
<tr>
<td>108 All</td>
</tr>
<tr>
<td>102 HF</td>
</tr>
<tr>
<td>100 Hacked</td>
</tr>
<tr>
<td>96 No-IP</td>
</tr>
<tr>
<td>95 test</td>
</tr>
<tr>
<td>84 Col334</td>
</tr>
<tr>
<td>58 Guest1</td>
</tr>
<tr>
<td>53 kurban</td>
</tr>
<tr>
<td>51 Victim</td>
</tr>
<tr>
<td>51 Test</td>
</tr>
<tr>
<td>49 User</td>
</tr>
<tr>
<td>48 Guest</td>
</tr>
<tr>
<td>47 Vitima</td>
</tr>
<tr>
<td>46 1</td>
</tr>
<tr>
<td>40 Slave</td>
</tr>
<tr>
<td>36 Hack</td>
</tr>
<tr>
<td>36 DOS</td>
</tr>
<tr>
<td>34 Guest17</td>
</tr>
<tr>
<td>32 DC</td>
</tr>
<tr>
<td>31 HACKED</td>
</tr>
<tr>
<td>27 Steam</td>
</tr>
<tr>
<td>27 RAT</td>
</tr>
<tr>
<td>26 server</td>
</tr>
<tr>
<td>26 Server</td>
</tr>
<tr>
<td>24 hack</td>
</tr>
<tr>
<td>23 all</td>
</tr>
<tr>
<td>23 DarkComet</td>
</tr>
<tr>
<td>23 BOT</td>
</tr>
<tr>
<td>22 darkcomet</td>
</tr>
<tr>
<td>21 Hacker</td>
</tr>
<tr>
<td>20 hacked</td>
</tr>
<tr>
<td>20 123</td>
</tr>
<tr>
<td>18 PC</td>
</tr>
<tr>
<td>18 KURBAN</td>
</tr>
<tr>
<td>18 BITS</td>
</tr>
<tr>
<td>16 lol</td>
</tr>
<tr>
<td>16 Victim</td>
</tr>
<tr>
<td>15 Rat</td>
</tr>
<tr>
<td>15 HACK</td>
</tr>
<tr>
<td>15 Bot</td>
</tr>
<tr>
<td>14 vitima</td>
</tr>
<tr>
<td>14 hak</td>
</tr>
<tr>
<td>14 VK</td>
</tr>
<tr>
<td>14 Solis</td>
</tr>
<tr>
<td>14 LOL</td>
</tr>
<tr>
<td>13 user</td>
</tr>
<tr>
<td>13 slave</td>
</tr>
<tr>
<td>13 CSGO</td>
</tr>
<tr>
<td>12 hot</td>
</tr>
<tr>
<td>12 TEST</td>
</tr>
<tr>
<td>12 HACKER</td>
</tr>
<tr>
<td>12 Gurban</td>
</tr>
<tr>
<td>12 Admin</td>
</tr>
<tr>
<td>12 111</td>
</tr>
<tr>
<td>11 vitime</td>
</tr>
<tr>
<td>11 NEW</td>
</tr>
<tr>
<td>11 Facebook</td>
</tr>
<tr>
<td>10 svchost</td>
</tr>
<tr>
<td>10 new</td>
</tr>
<tr>
<td>10 hacker</td>
</tr>
<tr>
<td>10 Vitimas</td>
</tr>
<tr>
<td>10 USER</td>
</tr>
<tr>
<td>10 Trolld</td>
</tr>
<tr>
<td>10 Testing</td>
</tr>
<tr>
<td>10 TestGuest</td>
</tr>
<tr>
<td>10 Skype</td>
</tr>
<tr>
<td>10 Omegle</td>
</tr>
<tr>
<td>10 Minecraft</td>
</tr>
<tr>
<td>10 LucidsVictim</td>
</tr>
<tr>
<td>10 Infected</td>
</tr>
<tr>
<td>10 Guest15</td>
</tr>
</tbody>
</table>
Sometimes interesting things come up

• JSocket Unique Campaign IDs by count

418 JSocket (DEFAULT)
  6 order
  6 lion
  6 amendmentcopy
  3 ThePunisher

3 August24rdBombing
  2 quotation
  2 onlyali
  2 festus
  2 admi
Sometimes interesting things come up

2004 Russian aircraft bombings

From Wikipedia, the free encyclopedia

The Russian aircraft bombings of August 2004 were terrorist attacks on two domestic Russian passenger aircraft at around 23:00 on 24 August 2004. Both planes had flown out of Domodedovo International Airport in Moscow.

Contents [hide]

1 Flights
   1.1 Volga-AviaExpress Flight 1353
   1.2 Siberia Airlines Flight 1047
2 Responsibility
3 Trials
4 References
5 External links
Digging deeper

© Fidelis Cybersecurity.  All rights reserved.
Digging deeper

host nikresut015js.zapto.org
nikresut015js.zapto.org has address 50.7.199.164

30058 | 50.7.199.164 | 50.7.192.0/19 | US | arin | 2010-10-18 | FDCSERVERS - FDCservers.net,US

RRset results for nikresut015js.zapto.org/ANY

bailiwick zapto.org.
count 11
first seen 2015-09-30 00:24:21 -0000
last seen 2015-10-08 11:37:34 -0000
nikresut015js.zapto.org. A 50.7.199.164
Digging deeper

• What’s the biggest byproduct of Big Data?

• Despite the ominous name, likely no connection to the bombing on 24 August.

• Without further review, marketing may have spun up a new “APT campaign” blog post.

• Just as important to have a large historical dataset to create and correlate backwards is the ability to prove an initial conclusion is wrong.
Correlating with Mutexes

- Some malware families randomly generate a mutex via the builder. Needed to prevent multiple copies of the same malware from running.

- 1867 ***MUTEX***
- 755 Pluguin
- 445 DC_MUTEX-F54S21D
- ......
- 26 DC_MUTEX-KT2FTNQ
- 23 DC_MUTEX-R0FHB8M
- 20 E4JR7ST81TYT8U
- 18 DC_MUTEX-V76C9X6
- 18 ***CryptoSuite***
- 17 DC_MUTEX-CNAFSEW
- 16 DC_MUTEX-RJ62AL7
- 16 DC_MUTEX-1FBMSBT
Correlating with Mutexes

```
# grep "DC_MUTEX-1FBMSBT" fullratdump.csv | awk -F "," '{print $3,$5,$7}'
```

DOS 12/12/15 20:46 asdssaaassss.ddns.net
DOS 12/9/15 18:03 91.225.73.26
DOS 11/28/15 17:07 46.119.218.223
DOS 11/14/15 16:11 46.119.218.223
DOS 11/14/15 11:48 46.119.227.6
DOS 11/13/15 12:59 46.119.227.6
DOS 11/3/15 13:10 134.249.20.28
DOS 11/2/15 2:50 134.249.20.28
DOS 11/1/15 15:53 134.249.20.28
DOS 9/30/15 2:01 sattorov.ddns.net
DOS 9/13/15 19:19 aleksej-morozov.noip.me
  8/18/15 6:38 pingvin.ddns.net
DOS 8/5/15 16:39 draken.zapto.org
DOS 7/23/15 9:18 zhbrcbnhfh.no-ip.org
DOS 7/15/15 10:17 test777test.ddns.net
DOS 7/7/15 8:31 5.248.21.138
The Ashley Madison Correlation Trick

• Password can authenticate victim and server, so often they change less even when other settings change. Unique password by count with PoisonIvy:

```
824  ""@client$321$"
228  ""admin"
20   ""administrator"
  9   ""80012345678"
  9   ""13800138000"
  9   ""13644713530"
  9   ""12345678901"
  6   ""version2013"
  6   ""teleport"
  5   ""sdjnga"
  4   ""boyyzj"
  3   ""dani10010"
  3   ""anonymous"
  3   ""80A80B80C80D"
  3   ""170077"
  2   ""pass@C2SV"
```
Points to three C2s:
- popkaka.xicp.net
- popkaka.xicp.net has address 174.128.255.227
- Running off Sharktech in US
- sg3appstore.net
- sg3appstore.net has address 121.127.234.170
- Running off Sun Network in Hong Kong
- us3appstore.net
- us3appstore.net has address 121.127.234.170
Technique can be used to feed DGAs

From Cert.PL malware ripper

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>binary</td>
<td>6eb749c3519e17f4051cbdd1de993cd2</td>
</tr>
<tr>
<td>rc4key</td>
<td>o2Jw73NaoZ837Yhe</td>
</tr>
<tr>
<td>base-domain</td>
<td>g0jdy3826yenz63om.cc</td>
</tr>
<tr>
<td>timestamp</td>
<td>2016-01-11 12:06:07</td>
</tr>
<tr>
<td>post-path</td>
<td>/go8dj37dh672bxj8j8ld/</td>
</tr>
<tr>
<td>cnc</td>
<td>g0jdy3826yenz63om.cc</td>
</tr>
<tr>
<td>botnet</td>
<td>262-N-L</td>
</tr>
<tr>
<td>public_key</td>
<td>-----BEGIN PUBLIC KEY----- MBITANBgkqhkG9w0BAQEFAAOCAQ4AMIIBCQCAQIB91wYsVb0vAY+YWQLUp3J vZujE6plNepLlx+bGSygnZW9yr5dk/K/Qcltj6cppkciif8kyM/HwP+QN2Fm7TpaO SoptSc8gk9i/8v3f7/kS51zDkJkMvleYOwlg7v43ZrdGwjeR22OBswcQE0TxRba5I skpaP6N/kStuM1UtHlYWmKCycaj9ix5izMy4N4bvw81ST0M5zGvmTJ9nAVzFf lXqZ9hw1vmwSIVhXqsVrPMtI9iIZ56Tu1ARbsxJg0iLORrn2vVZ57/wScQIr+F+G bhXny1rLVvm/be0n0NpFJNpFSJ6D02ysl/GVn2fif7edxeBThbRjiqQFSMFex.AgMBAAE= -----END PUBLIC KEY-----</td>
</tr>
<tr>
<td>type</td>
<td>tinba_dga</td>
</tr>
<tr>
<td>tld</td>
<td>com.net.in,ru</td>
</tr>
</tbody>
</table>
Resolving Hostnames (May 2015 - now)

Hostname Resolution

Resolved
NXDOMAIN
RFC 1918 Address
0.0.0.0
The need for constant surveillance

• DNS resolving is point-in-time, may resolve sometimes and sometimes not.
  • The fact that it doesn’t resolve in and of itself is not a contraindication.
• Some configs may be garbage.
  • Some RATs, for instance, were configured to beacon to the IP 8.8.8.8
• DNS is under control of attacker, even if they engage in deception, detecting that has intelligence value.
• Some malware uses encoded IPs.
  • i.e. resolved IP is then “converted” to real IP.
Domain Generation Algorithms

- Usually a complex math algorithm to create pseudo-random but predictable domain names.

- Now instead of a static lists, you have a dynamic list of hundreds or thousands of domains and adversary only needs to have a couple registered at a time.

- Can search for “friendly” registrars to avoid suspension.

- Can engage in counter-intelligence.
Counterintelligence – or worse version

- What if adversary knows you resolve these DGA domains and put directly into your firewall (and I know people do this with my feeds)?

- Anyone recognize these IP addresses? They are the DNS Root Servers

198.41.0.4
192.228.79.201
192.33.4.12
199.7.91.13
192.203.230.10
192.5.5.241
192.112.36.4
128.63.2.53
192.36.148.17
192.58.128.30
193.0.14.129
199.7.83.42
202.12.27.33
Counterintelligence – or worse version

- Taking action on information without analysis is generally a bad idea, especially when the information is under the complete control of the adversary.

- This is why intelligence analysis is so important.

- (I whitelisted the root servers after I noticed an adversary tried to do an attack similar to this.)
Types of DGAs

- Almost all DGAs use some time of “Seed”.
- Types:
  - Date-based
  - Static seed
  - Dynamic seed
- Seed has to be globally consistent so all victims use the same one at the same time.
Other DGA Hardening Techniques

- Choice of gTLD matters.
  - Some doing have WHOIS protection, make it hard to sinkhole

- Rotation of seeds

- Some malware has rudimentary “sinkhole awareness”

- Adversarial objectives: Maintain control, limit surveillance
Examples of select DGAs - Cryptolocker

- Used 1000 domains a day across 7 gTLDs. Order domains are queries in based on `GetTickCount()`
- Eerily similar to DGA described in Wikipedia article on DGAs.
- Used previously by Flashback OSX Worm.
- Never changed during the life of the malware campaign.
- Successfully taken down in June 2014
Examples of select DGAs - Tinba

- Generated 1,000 domains a day, not date-seeded.

- Seeded by an initial hostname and a defined gTLD (one or more).

- Changes seeds often and tends to update already infected machines.
  - At least sinkholing tended to be ineffective for more than a few days.
Examples of select DGAs - Bedep

- Uses a dynamic seed – currency exchange values for foreign currency
  - European Central Bank produces daily feeds of the rates, this is used as source data.

- Impossible to predict in advance even though code to generate the domains is publicly available.
What the use of DGAs gives the good guys

- Easy ability to sinkhole unused DGA domains to gather additional intelligence.
- Easier ability to do bulk takedowns.
  - *IF* you can predict domains in advance.
- The ability to surveil malicious infrastructure in near real-time.
What the use of DGAs gives the good guys

- The use of DNS in malware severely limits the ability of the adversary to play games.
  - They need the world to be able to find their infrastructure in order to control victim machines.

- Even when DGA changes, the adversary **tends** not to immediately change their infrastructure too.
  - Allows for the use of passive DNS to see the extent of DGA changes.
DGA surveillance

- Pre-generate all domains 2 days before to 2 days in future.

- Pipe all those domains into adnshost using parallel to limit the number of lines.

- Able to process over 700,000 domains inside 10 minutes (and I’m not done optimizing).

  - `parallel -j4 --max-lines=3500 --pipe adnshost -a -f < $list-of-domains | fgrep -v nxdomain` `>> $outputfile`
Example

2n2qlh5hqcrwvo.net,8.5.1.40,dns1.name-services.com|dns2.name-services.com|dns3.name-services.com|dns4.name-services.com|dns5.name-services.com,98.124.192.1|98.124.193.1|98.124.194.1|98.124.196.1|98.124.197.1,M aster Indicator Feed for bebloh non-sinkholed
lvzyjwj1fakh55i.com,208.91.197.113,ns1.dynadot.com|ns2.dynadot.com,54.164.135.208|54.164.162.213|54.165.100.140|54.68.142.171|54.68.143.189|54.68.145.110|54.68.55.168|54.88.182.181,M aster Indicator Feed for bebloh non-sinkholed
evtzxdehixfrktsjy.com,188.138.25.129,ns1.regway.com|ns2.regway.com,109.70.27.118|194.226.96.118,M aster Indicator Feed for bedep non-sinkholed
ifamvhlimcaezy.com,188.138.125.65,ns1.regway.com|ns2.regway.com,109.70.27.118|194.226.96.118,M aster Indicator Feed for bedep non-sinkholed

Public Feeds at: http://osint.bambenekconsulting.com.feeds
This is the C2-Master feed.
Surveillance is nice, what about notification?

- Creation of feeds and intake is still a passive tactic.

- It is all possible to automate notifications when key changes happen to allow for more near-time actions.

- This uses the Pushover application (Apple and Google stores) which has a very simple API.
New Dyre domain registered

OSINT-DYRE

From OSINT-DYRE on 8/13/15 at 7:05 PM

New dyre domain notification from:
osint.bambenekconsulting.com

g3bb703a8d7b99b19c8af8ac1b98280f67.tk

IPs:
195.20.40.235: NL, Netherlands

Nameservers:
d.ns.tk
c.ns.tk
b.ns.tk
a.ns.tk

Nameserver IPs:
d.ns.tk has address 194.0.41.1
c.ns.tk has address 194.0.40.1
b.ns.tk has address 194.0.39.1
a.ns.tk has address 194.0.38.1
New Bedep Domain Registered

From OSINT-BEDEP on 8/12/15 at 7:09 PM

New bedep domain notification from:
osint.bambenekconsulting.com

nrqagzfcnneozu.com

IPs:
5.135.16.204: FR, France

Nameservers:
ns1.regway.com
ns2.regway.com

Nameserver IPs:
ns1.regway.com has address 109.70.27.118
ns2.regway.com has address 194.226.96.118

Registrar: DOMAINCONTEXT, INC.
Whois Registrar Intel

- Often actors may re-use registrant information across different campaigns. There may be other indicators too.

- Sometimes *even with WHOIS privacy protection* it may be possible to correlate domains and by extension the actor.

- Most criminal prosecution in cybercrime is due to an OPSEC fail and the ability to map backwards in time of what the actor did to find that fail that exposes them.
Whois Info

- Many actors will use WHOIS protection… some just use fake information.

- “David Bowers” is common for Bedep.

- `ubuntu$ grep "David Bowers" *.txt | grep Registrant`

- `whois-bfzflqejohxmq.com.txt:Registrant Name: David Bowers`
- `whois-demoqmfritwektsd.com.txt:Registrant Name: David Bowers`
- `whois-eulleltnryrxagvokz.com.txt:Registrant Name: David Bowers`
- `whois-lepnzsiqowk94.com.txt:Registrant Name: David Bowers`
- `whois-mhqfmrapcgphff4y.com.txt:Registrant Name: David Bowers`
- `whois-natrkhkylqoxjtqt45.com.txt:Registrant Name: David Bowers`
- `whois-nrqagzfcnneouzo.com.txt:Registrant Name: David Bowers`
- `whois-ofkjmtvsnmy1k.com.txt:Registrant Name: David Bowers`
<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Date</th>
<th>Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>029uhbdfisjdj4.in</td>
<td>2015-02-25</td>
<td>--</td>
</tr>
<tr>
<td>298dkoaldjfiow-yets.in</td>
<td>2015-03-18</td>
<td>--</td>
</tr>
<tr>
<td>37aodjdopcoi.in</td>
<td>2015-03-17</td>
<td>--</td>
</tr>
<tr>
<td>37kdospwmeop.in</td>
<td>2015-03-25</td>
<td>--</td>
</tr>
<tr>
<td>3875jnciosprk.us</td>
<td>2015-03-31</td>
<td>--</td>
</tr>
<tr>
<td>394iopwekmicopw.com</td>
<td>2015-01-19</td>
<td>DOMAINCONTEXT, INC.</td>
</tr>
<tr>
<td>781zjpaosieu.in</td>
<td>2015-05-07</td>
<td>--</td>
</tr>
<tr>
<td>7u2yopwjh.in</td>
<td>2015-05-07</td>
<td>--</td>
</tr>
<tr>
<td>82hasyqtwq.in</td>
<td>2015-05-13</td>
<td>--</td>
</tr>
<tr>
<td>82kolesan.in</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>a4egjph0jy.us</td>
<td>2015-07-25</td>
<td>--</td>
</tr>
<tr>
<td>aachurill.com</td>
<td>2015-04-30</td>
<td>DOMAINCONTEXT, INC.</td>
</tr>
<tr>
<td>aachurill.in</td>
<td>2015-04-22</td>
<td>--</td>
</tr>
<tr>
<td>ablooovades.com</td>
<td>2015-03-04</td>
<td>DOMAINCONTEXT, INC.</td>
</tr>
<tr>
<td>abozpkiowew28a9.in</td>
<td>2014-12-08</td>
<td>--</td>
</tr>
<tr>
<td>absuawpchiwkhj8.com</td>
<td>2015-04-19</td>
<td>DOMAINCONTEXT, INC.</td>
</tr>
<tr>
<td>ac38vplik8p.com</td>
<td>2015-07-10</td>
<td>DOMAINCONTEXT, INC.</td>
</tr>
<tr>
<td>accident-muscle.com</td>
<td>2015-03-05</td>
<td>DOMAINCONTEXT, INC.</td>
</tr>
<tr>
<td>ace-nate-rade.in</td>
<td>2015-03-24</td>
<td>--</td>
</tr>
<tr>
<td>aederradpow.in</td>
<td>2014-10-13</td>
<td>--</td>
</tr>
<tr>
<td>adgesiklopatws</td>
<td>2015-02-27</td>
<td>PDR Ltd. d/b/a PublicDomainRegistry.com</td>
</tr>
<tr>
<td>adoncorst.com</td>
<td>2015-04-29</td>
<td>DOMAINCONTEXT, INC.</td>
</tr>
</tbody>
</table>
Wrapping it up

• Both techniques can be used to observe adversary behavior outside an organization to get a fuller picture of what they are involved in.

• Using this you can proactively have elements needed to proactively block potential adversaries or to end feed a hunt team.

• Techniques can be used to disrupt their operations even if they aren’t actively targeting you.

• Key is to remember to go through the time consuming exercise of doing real intelligence work instead of pumping into firewalls/IPS.
QUESTIONS?

THANKS TIM LEEDY AND THE REST OF MY TEAM. KEVIN BREEN, MANY OTHERS.

JOHN BAMBENEK
JOHN.BAMBENEK@FIDELISSECURITY.COM
/JCB@PEOPLE.OPS-TRUST.NET
+1 217 493 0760

DGA FEEDS:
OSINT.BAMBENEKCONSULTING.COM/FEEDS/